CrowdStrike and Cloudflare

Enrich Zero Trust with easy creation of device-based access policies, making connections to corporate resources safer, faster, and more seamless for end users

Challenge

Today users, devices, and applications largely exist outside the traditional corporate perimeter. Traditional tools that connect employees to corporate applications (like VPNs and IP-based controls) grant excessive trust, exposing users to malicious threats like data loss, phishing, and malware. They can also increase an organization's attack surface, limit visibility, and frustrate end users. Zero Trust Network Access (ZTNA) and Secure Web Gateway (SWG) are safer, faster, and easier ways to enable access for increasingly distributed workforces. Cloudflare Zero Trust protects critical resources, and users are granted access after verifying the identity, context, and policy adherence of each request. Adopting device posture in particular is a critical step and an important contextual signal for setting up effective Zero Trust policies.

Solution

Cloudflare and CrowdStrike have partnered to make it easy for organizations of all sizes to build Zero Trust policies based on CrowdStrike's Zero Trust Assessment (ZTA) score — a continuous real-time security posture assessment across all endpoints in an organization. This enables organizations to enforce conditional access and gateway policies based on device health and compliance checks to mitigate risks posed by compromised or malicious devices.

As these policies work across our entire Zero Trust platform, organizations can use them to build powerful rules invoking Browser Isolation, Tenant control, Anti-virus, or any part of their Cloudflare deployment.

- **Zero Trust Network Access (ZTNA)**: Cloudflare's ZTNA solution secures applications with identity, device, and context-driven rules. Our integration with the CrowdStrike Falcon platform allows mutual customers to build conditional access policies that require a minimum ZTA score is met before a user is granted access.
- **Secure Web Gateway (SWG)**: Cloudflare SWG protects users and data safe from threats on the Internet, with no backhauling required. Through our integration with CrowdStrike, organizations can leverage the device context offered by CrowdStrike's ZTA score to influence various mitigation or protection measures.

Benefits

Cloudflare and CrowdStrike's partnership helps customers identify, investigate, and remediate threats quickly, and ensures security for external, public-facing web properties and internal resources.

Easily enforce device-aware access policies with a few clicks in the Cloudflare dashboard

Prevent lateral movement of infected devices, restricting them from accessing sensitive data (e.g. account credentials).

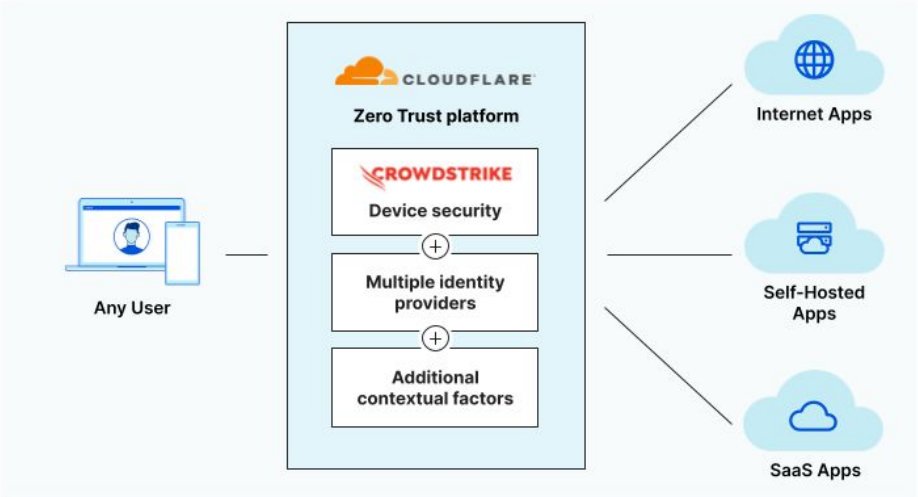
Cloudflare's lightning-fast network brings enforcement decisions within 50ms of 95% of the world's Internet-connected population

Integration Overview

With this integration, organizations can build on top of their existing Cloudflare Access and Gateway policies ensuring that a minimum ZTA score has been met before a user is granted access. If a user does not meet the threshold ZTA score, the administrator can choose to block, isolate, and run other checks.

Zero Trust Assessment (ZTA)

Cloudflare customers can build Zero Trust policies based on the presence of a CrowdStrike agent at the endpoint and its Zero Trust Assessment (ZTA) score. This score delivers continuous, real-time security posture assessments across all endpoints in an organization regardless of location; enables the enforcement of conditional access based on device health and compliance checks to mitigate risks; and is evaluated each time a connection request is made, making conditional access adaptive to the evolving condition of the device.



Access request
The user requests access to an application

Zero Trust verification
Cloudflare verifies request on the basis of the CrowdStrike agent and its attributes, the user's identity, and other contextual factors

Access granted
The user is granted access to the resource only after verifying policy adherence

How to Configure the Integration

There are three steps to enable Cloudflare and CrowdStrike's integration:

1. First, customers using Cloudflare Zero Trust suite will need to add Crowdstrike as a **device posture provider** in the Cloudflare Zero Trust dashboard (*Settings* → *Devices* → *Device Posture*).

2. After adding CrowdStrike as a device posture provider in the Cloudflare dashboard, customers can **create specific device posture checks** requiring users' devices to meet a certain threshold of ZTA scores.

3. These rules are then used to create conditional Access and Gateway policies to **allow or deny access to applications, networks, or sites**. Administrators can choose to block or isolate users or groups with malicious or insecure devices.

About CrowdStrike

CrowdStrike Holdings, Inc., a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value. Learn more at crowdstrike.com.

About Cloudflare

Cloudflare Zero Trust is a security platform that increases visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, user traffic is verified, filtered, inspected, and isolated from Internet threats; and performance never suffers, as users connect through data centers near them in 250+ cities and 100+ countries around the world. Other Zero Trust providers offer multiple point products to protect from every threat vector, but leave customers to manage their own attack surface. The Cloudflare platform stops more attacks by isolating applications and endpoints from the attack surface by shifting it to our edge, and applies threat defenses to shield that edge. Learn more at cloudflare.com/products/zero-trust.